HPE Security Fortify Software Update (Patch) Version 16.11 Released

This VA Software Assurance Notification is an announcement about the release of updated HPE Fortify Static Code Analyzer (SCA) software. Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP, and enforced as part of the ATO issuance process.

The most recent version of Fortify, and the complete, most recent set of the Fortify rulepacks must be used when scanning code. This patch fixes critical performance issues identified in Fortify SCA 16.10 and can be downloaded by current VA Fortify license holders by requesting access to a location on the internal network by sending an email to OISSwASupportGroup@va.gov

Fortify scans that do not use this new release of the Fortify software will result in scan issues for secure code review validation submission packages accepted* after August 8, 2016. Accepted is defined as all required secure code review validation prerequisites have been met. For information about requesting secure code review validations, please see here.

Issues fixed in HPE Security Fortify Static Code Analyzer 16.11

- Fixed: Decline in SCA scan time performance for JS projects
- Fixed: SCA reported errors and warnings while parsing some syntactically correct VB6 source code.
- Fixed: MSBuild Integration in SCA now supports directory paths that contain spaces.
- Added: Support for changes in the behavior of Xcode between versions 6.2 and 6.3
- Improved support for C++ and Objective-C++ in Xcode projects
- Added: Support for specifying custom xconfig files for objective C in the command line
- Improved support for Swift 2.2
- Added: Support for .fpr file names in languages that use non-ASCII characters
- Fixed: Invalid SCA warnings for unresolved ENUM values in Java Switch construct
- Changed: A change has been made to how SourceAnalyzer resolves JAVA classes with the same name. Previously, sourceanalyzer would use the last loaded class for resolution purposes, and the new behavior is to use the first loaded class.

  Suppose A.jar and B.jar both contain Data.class. If sourceanalyzer is invoked this way:

  $ sourceanalyzer -classpath A.jar:B.jar source.java

  - Prior to this release, sourceanalyzer used the last loaded class when deciding which version of a class to use. The copy of Data.class in B.jar would be used.
  - In 16.11 and above, sourceanalyzer uses the first loaded class when deciding which version of a class to use. Data.class from A.jar would be used

- Fixed: SCA produced IndexOutOfBounds exception when jar file was passed to JavaBootCLasspath while analyzing any Java file
- Fixed: SCA threw unresolved function call error when scanning a Java/JSP project employing Spring Security
- Fixed: False positives around String.Empty syntax
- Fixed: SCA reported an ‘Unable to parse T-SQL’ error for valid TSQL syntax
- Fixed: Null pointer exception with ASP.Net source code
- Fixed: SCA produced an error when C++ lambdas were passed to Objective-C message handlers declared to receive blocks

Issues fixed in HPE Security Fortify Static Code Analyzer Tools 16.11

- Fixed: MSBuild task now handles spaces correctly
- Fixed: Fortifyupdate now uses the correct URL when updating security content from SSC
- Fixed: Locating .NET source code in FPRs generated by older sourceanalyzer versions now handles system dependent file delimiters
- Fixed: Merging FPRs from older SCA versions with 16.10 FPRs now behaves correctly